Le chiffrement des données
XOR

1. L'opérateur XOR

L'opérateur logique XOR (ou exclusif) est noté ⊕.

- **Table de vérité** de l'opérateur XOR entre deux bits E1 et E2 (ci-contre).
- **Propriété de XOR** : soit trois nombres entiers x, y et z (codés sur 8 bits par exemple) tels que **x ⊕ y = z** alors on a aussi : **z ⊕ x = y** et **z ⊕ y = x**.

E1	E2	S
0	0	0
0	1	1
1	0	1
1	1	0

Fig 1 : table de vérité du XOR

2. Le chiffrement XOR

Cette méthode repose sur l'opérateur logique XOR et sur la répétition d'une clé alphanumérique.

La propriété du XOR va permettre de chiffrer et de déchiffrer un message de la même façon. Pour déchiffrer un message chiffré par un XOR, il suffit de réaliser un XOR avec la clé qui à servit à chiffrer le message.

2.1. Méthode de chiffrement

Chaque caractère du message et de la clé est représenté par un entier, le code ASCII.
Ce nombre est lui-même représenté par un nombre binaire à huit chiffre (bits).

- La clé est placée en dessous du message à coder, en la répétant autant de fois que nécessaire.
- Le message et la clé sont convertis en binaire (en passant par le code ASCII).
- Le message chiffré est obtenu en réalisant un XOR bit à bit (il peut être reconverti en caractère ASCII).

2.2. Méthode de déchiffrement.

En utilisant la propriété du XOR, il suffit de réaliser un XOR entre la clé et le message chiffré pour obtenir le message en clair.

2.3. Exemple

Le mot MESSAGE est converti en binaire.

Lettres	M	E	S	S	A	G	E
ASCII	**4D**	**45**	**53**	**53**	**41**	**47**	**45**
Binaire	**0100 1101**	**0100 0101**	**0101 0011**	**0101 0011**	**0100 0001**	**0100 0111**	**0100 0101**

Le mot CLE en binaire donne : **0100 0011 0100 1100 0100 0101.**

Message en binaire	**0100 1101**	**0100 0101**	**0101 0011**	**0101 0011**	**0100 0001**	**0100 0111**	**0100 0101**
Clé en binaire (répétée si besoin)	**0100 0011**	**0100 1100**	**0100 0101**	**0100 0011**	**0100 1100**	**0100 0101**	**0100 0011**
Message chiffré en binaire	**0000 1110**	**0000 1001**	**0001 0110**	**0001 0000**	**0000 1101**	**0000 0010**	**0000 0110**

Bob a donné rendez-vous à Alice dans le centre bourg de la commune figurant sur son message chiffré. Bob lui a transmis la clé (0101 1100 0111 1000) pour trouver cette commune.
✍ Aider Alice à trouver la commune du rendez-vous.

Message chiffré en binaire	**0000 1111**	**0001 1001**	**0010 1110**	**0000 0010**	**0011 1001**	**0001 1001**	**0010 1001**
Clé en binaire							
Message déchiffré en binaire							
ASCII							
Commune							